Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 5, Issue 1; January-March, 2018, pp. 7-12

http://www.krishisanskriti.org/Publication.html

Copy-Move Forgery Detection Using Stationary Wavelet Transform and SIFT

Ritu Agarwal[1] and B.N. Deepankan[2]

[1,2]Delhi Technological University
E-mail: [1]ritu.jeea@gmail.com, [2]bn.deepankan@gmail.com

Abstract—*With the increasing availability of the various image editing software and algorithms, tampering of images can be done easily and it has become a difficult task to differentiate between an authentic image and a tampered image. Our focus is on a special type of image forgery which is a copy-move forgery. Where one region of the image is copied into another region of the same image in order to create a fake scene depicts an original image. We have shown a new method for the copy-move forgery detection, by using Stationary Wavelet Transform (SWT), which is unlike DWT is shift-invariant and SIFT is used for feature extraction which is invariant to transform, scale, rotation, and noise. Several results have been shown that our proposed method performs efficiently in the detection of copy-move forgery.*

1. INTRODUCTION

Since every information we get in our day to day life has been in a digital form with increasing technological advancement, it has brought a major issue of security. With the latest development of powerful algorithms and technology for manipulating digital images has made a very difficult task for determining the authenticity and integrity of the original image.

The Digital Image can be manipulated using many techniques and software like transformation, scaling, filtering, cropping, blurring, photoshop, coral draw, and others. Image forgery has indeed become a major challenge for institutions as well as individuals. The verification of digital image is necessary for many applications such as forensic, media, glamour, military, scientific, etc.

Such kind of rapid increase in the field of image forging prompts us to understand the intricate differences between an authentic and a forged image. In order to answer such questions from a forensics perspective, original image authenticity has been traced from where it has been created. In the past decade confirming the authenticity of the mage has become a major area of focus and it increases various methods that have been developed for detecting the forged image and original image. Digital Image forgery can be detected using two different approaches. These are active approach and Passive approach. The active approach is of two types, one is watermarking and another is steganography. The basic idea of watermarking is to embed some information in digital images so that it cannot be misused or owned by others and to check the authenticity of the message. Steganography is the technique to hide a message within a digital image, to protect the privacy of the data.

The Passive approach doesn't require any prior information about the image as it can examine the image for any traces of manipulation during the preprocessing step. With the help of different image forgery detection techniques the forged area, location and the amount of forgery can be detected. It includes copy-move forgery and image splicing and they also help to detect the operations that occur, like rotation scaling, blurring, etc.

In this paper, we present an efficient algorithm for the detection of image forgery which is invariant to transform, scale, rotation, and noise. The third section gives a detailed explanation of our approach and the seventh section shows the experimental results.

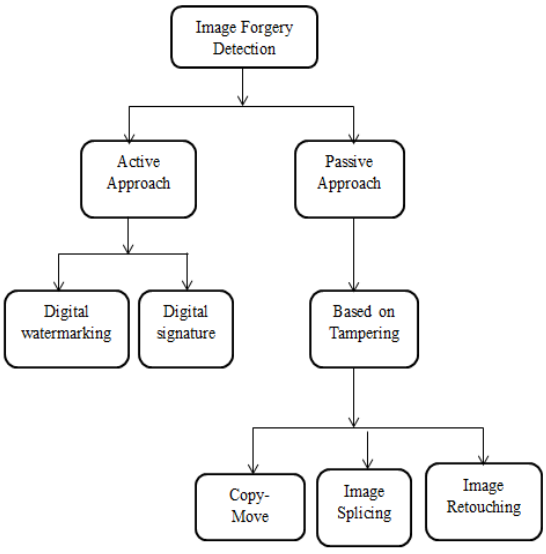

Figure 1: Different types of Image forgery.

2. RELATED WORK

With the various image editing software, tempering an image has become easier. There are many different techniques has been proposed for the detection of the forgery. [1] uses a hybrid approach which involves DWT with DCT. In this approach consider a grayscale image or convert a color image into a grayscale image and apply DWT to divide the image into sub-images. Slide a window of size n x n over those sub-images resulting in K blocks. DCT (QD) is applied on the rows of the blocks to reduce the vector length and a matrix is formed H. The matrix is lexicographically sorted and Normalized shift vector is calculated for the matched pairs and it is compared with the user-defined threshold to determine if the region is being copied.

In [2] approach Dyadic Wavelet Transform is used i.e. DyWT. Apply DyWT on the image to get LL^2 and HH^2 sub-bands. Analyze the pattern for each segment, and calculate the Euclidean between the pair of patterns. Check if the distance is less than the threshold T. If yes, then that region is marked as forged. [3] has proposed an approach which involves SURF and DyWT, which is identical to SURF and DWT but DyWT is used as DWT is not shift-invariant. In this approach DyWT is performed into an image which divides the image into sub-images, key points and features are extracted by applying SURF. Feature descriptor vector of SURF is obtained and determine the similar feature descriptors. Finally, mark the forged regions.

[4] proposed a keypoint technique by using SIFT. SIFT involves four major step first, Scaled spaced extrema detection which finds the interest points using Laplacian of Gaussian (LOG). Second, key points are selected based on the measures of their stability. Third, Depending on the scale, a neighborhood point is chosen around the keypoint location. Then for that region, the gradient magnitude and direction is calculated. Fourth, a 16x16 neighborhood is selected near the key point and it is separated into 16 sub-blocks of 4x4 size. Then, the Key point between similar image is matched.

In [5] presented an algorithm for tampering detection using SVD. A small window of size B x B is slid over the input image to separate the image into overlapping blocks. SVD is applied to these separated blocks to obtain feature vectors, sort them and store it in the matrix. k-d tree is constructed using the feature vectors and it is searched for similar blocks. The matched blocks satisfying a threshold t will be labeled as suspected regions and these suspected regions are merged together to determine the tampered region. [6] proposed an algorithm involving local binary pattern and neighborhood clustering. In this algorithm the colored image is divided into R, B and G color components and these components are divided into blocks. LBP histogram is extracted for each component and calculate the distance between blocks using histogram for every component. Then, sort the block-pairs according to the minimum distance and keep only the shortest one-fourth of the total. Extract block pairs which are common in the three components, if duplicates were found then create sub-blocks using clustering and should a visual result. [7] presented a robust and efficient technique in which it involves a block of size a x a is slid over the image to divide it into coinciding blocks, and seven characteristic features are calculated for each block C_j (j=1,2,3…7) where C_1, C_2, and C_3 red, green and blue components. C_4, C_5, C_6, and C_7 are the characteristics feature of Y channel which is a combination of R, G and B. These characteristic features are stored in a vector V for each block separately and saved in an array A. The array A is lexicographically sorted and similarity is calculated between two vectors if it is greater than a threshold L it is recorded. A histogram is prepared with the recorded vectors, greater than threshold L and choose the main vector, d if any vector differs too much from d, it is discarded and remaining vectors are put in a binary image with the forged region set to white and rest of the region is set to black. [8] proposed an algorithm for both keypoint regions and smooth regions. Initially, Simple Linear Iterative Clustering [9] is applied to the image to separate the image into different blocks. Then SIFT is used to extract a key point from each block, the number of key points in a region is divided by the total number of pixels in that region to determine if it is a smooth region or a key point region. If it is detected as a key point region then the duplicate part is marked by using multiple keypoint matching [10] and RANSAC [11] is used to filter outliers. If it is a smooth region then Zernike moments [12] is used to detect the copied part.

With the above discussion, we can conclude that there are several methods for the detection of the forged region.

Figure 2. Original Image.

Figure 3. Forged Image.

3. THE PROPOSED APPROACH

In this paper, we presented a new algorithm for detection of the forged region. Initially, SWT is applied to the input image to separate the image into different wavelet domain such as LL, LH, HL, and HH. SIFT is applied on the LL part of the resulted image and key points are extracted because LL part consists of the most of the information. Finally, matching between the similar key-point descriptors are made to detect any tampered region.

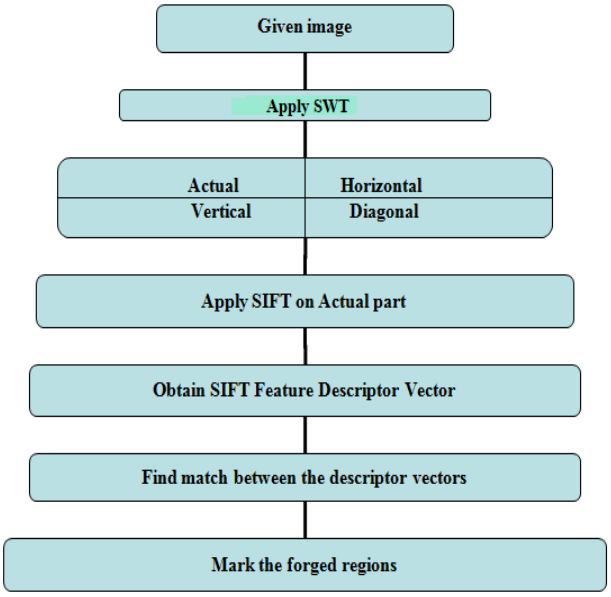

Figure 4. The Proposed Approach.

4. STATIONARY WAVELET TRANSFORM

In related work, there are many techniques where the forged image is detected using discrete wavelet transform (DWT), but DWT is not shift-invariant and it is not optimal for analysis of data. SWT [13] is used to overcome the problem of DWT as it is shift-invariant, because of this property vector coefficients doesn't shrink between scales like in DWT. Also, SWT is capable of performing the efficient edge detection, those images which contain duplicate regions which are blurred along the edges can also be easily detected. SWT can also be applicable to any arbitrary size of discrete (image) signals. But DWT can only apply to the dimensions in power of 2.

Translation invariance or shift invariance obtained by removing upsamplers and downsamplers in the DWT and upsampling the filter coefficients by a factor of $2^{(j-1)}$ in the j^{th} level of the algorithm.

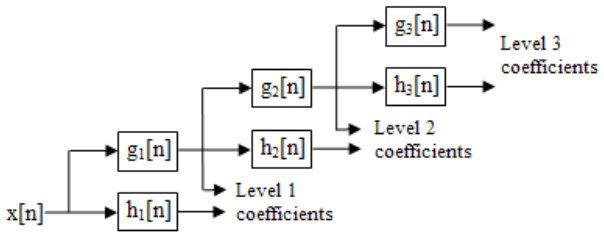

Figure 5. 3 Level SWT filter.

In our approach, we apply SWT to the image and separate the image into different wavelet domains such as LL, LH, HL, and HH.

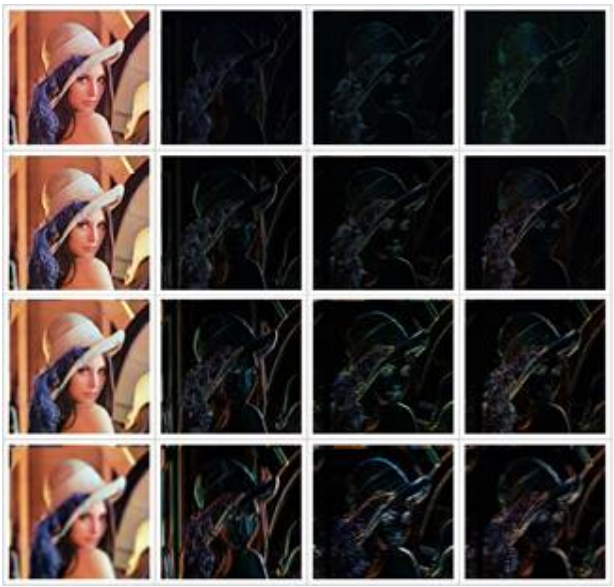

Figure 6. SWT applied to sample image.

5. SCALE INVARIANT FEATURE TRANSFORM

Every image contains key point features which don't change even if an image scaled, transform or rotated. These Key point can be used to distinguish an image from similar images. Here we use SIFT to detect those key points features of an image because it can efficiently detect the key points if the image is rotated or scaled. Also, SIFT doesn't get much affected by noise in an image. SIFT is a four-step filtering approach.

1) Scale-Space extreme detection. In this step difference of Gaussian (DoG) is used to detect the key points in an image. When the DoG is found then the image is searched for local extrema over scale and space. For eg. Each pixel is searched with its 8 neighbor pixels and also with 9 pixels in next scale and 9 pixels of the previous scale. If it is a local extremum then it is a key point.
2) Key-point localization. Refinement of the selected key points is done for more accurate results. Refinement is done by using the Tyler series expansion of scale space. If

the intensity of the selected key point is less than the threshold value (usually 0.03) then that key point is discarded. Due to the higher response of edges by DoG, it should be removed, so Harris corner detector is used. It uses a 2 x 2 Hessian matrix for calculation of the principal curvature.

3) Orientation assignment. Each key point is assigned an orientation based on calculating the gradient and magnitude of the neighborhood of each key point to achieve invariance for image rotation. It increases the stability in the matching of key points.
4) Key point descriptor. Now Key point descriptor is calculated by selecting the neighborhood key points of the candidate key point and further, it is separated into blocks. For each block, the histogram is created which also depicts the vector representation of the key point descriptor.

6. KEYPOINT MATCHING

Key point matching is done between two similar key points. Sometimes a match between two similar key points may vary on the second closest match due to noise or any other factor. For those cases a ratio between the smallest and the second smallest distance is taken if it is greater than 0.8 then they are rejected otherwise it is selected.

7. EXPERIMENTAL RESULTS

The proposed algorithm is implemented on MATLAB 2017a using MATLAB image processing toolbox. Where the implemented algorithm is tested with the database MICC-F220 [14] which consists of both authentic image and forged image.

Performance of an algorithm can be calculated in terms of precision, accuracy, and recall. Accuracy is equal to the ratio of the sum of tampered images detected with authentic image divided by the sum of all the results found during the detection process. Precision is the percentage of tampered images detected by the total sum of the tampered image and authentic image detected. The Recall is the percentage of the tampered image detected by the total sum of tampered images detected and the authentic images are detected as forged.

Figure 7. Forgery Detection.

Figure 8. Rotation attack.

Figure 9. Rotation and Scaling attack.

Some of the few terms used for calculations are:

1) TP (True Positive): Tampered image is detected.
2) FP (False Positive): Authentic image is detected tampering.
3) TN (True Negative): Authentic image is detected as the authentic image.
4) FN (False Negative): Tampered image is found authentic.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

We have taken some of the previous existing techniques such as the hybrid approach of DWT-SIFT [15], DWT-SURF and some key point based forgery detection methods such as SIFT and SURF. These methods are compared with our proposed technique.

Table 1: Comparison with existing techniques.

S. No.	Method	Precision (%)	Recall (%)	Accuracy (%)
1	DWT-SIFT	92.1	83.9	87.27
2	SIFT	95	74	85.4
3	SURF	78	70	75
4	DWT-SURF	77	64	72.6
5	SWT-SIFT	91	83.4	88.1

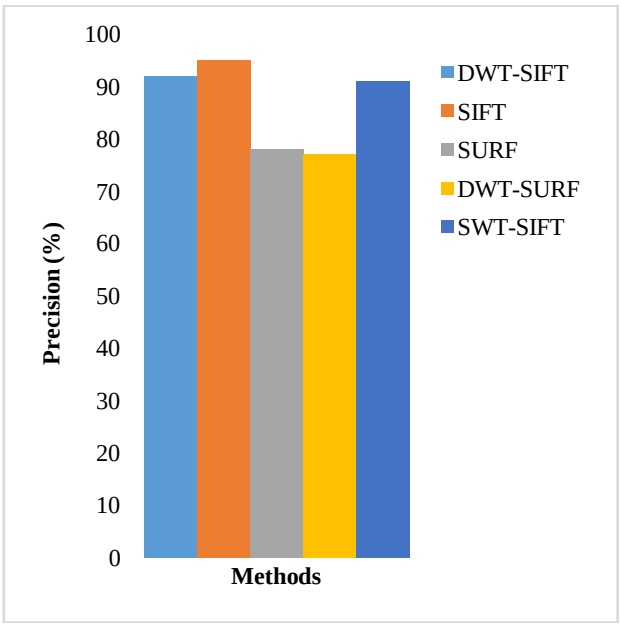

Figure 10. Graphical comparison of Precision between different methods.

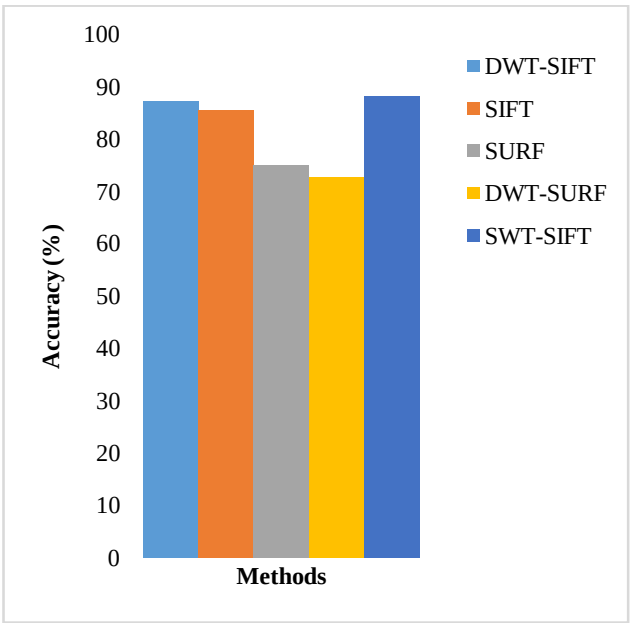

Figure 12: Graphical comparison of Accuracy between different methods.

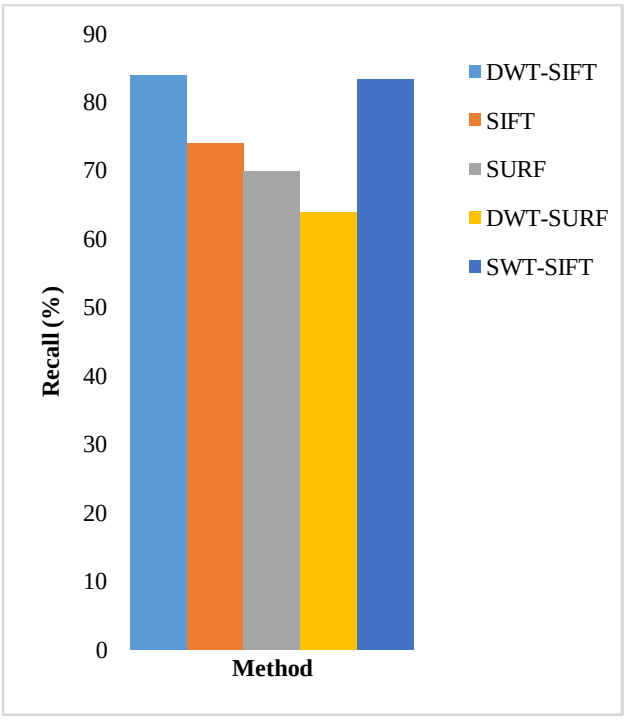

Figure 11: Graphical comparison of Recall between different methods.

Figure 13. Tampered Image

Figure 14. Forged part detected

In figure 13 we have shown the process of a proposed method for detecting the forgery. Initially, we have applied SWT and divide them into different wavelet domain and SIFT is applied to LL part. We have got a total of 5122 key points on that image, with 38 matches. Thus, we can say that the image is being tampered.

8. CONCLUSION

We can conclude that our proposed algorithm by using Stationary Wavelet Transform with SIFT can detect the forged image. Also, it is robust to different types of pre-processing that can be done to the image like scaling, transform and rotation. SWT ability of shift-invariance and not downsampling of the image can overcome the problems of

DWT. SIFT is useful in extracting key points from the image and matching similar features to determine if the image has been forged. We also have compared with different existing algorithms and found our proposed method has the highest accuracy among all and ours is the most feasible one.

REFERENCES

[1] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," *2011 18th International Conference on Systems, Signals, and Image Processing*, Sarajevo, 2011, pp. 1-4.

[2] N. Muhammad, M. Hussain, G. Muhammad and G. Bebis, "Copy-Move Forgery Detection Using Dyadic Wavelet Transform," *2011 Eighth International Conference Computer Graphics, Imaging and Visualization*, Singapore, 2011, pp. 103-108.

[3] M. F. Hashmi, V. Anand and A. G. Keskar, "A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms," 2014 *International Conference on Computer and Communication Technology (ICCCT)*, Allahabad, 2014, pp. 147-152.

[4] Alamro, Loai & Yusoff, Nooraini. (2017). Copy-move forgery detection using integrated DWT and SURF. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*. 9. 67-71.

[5] S. Prasad and B. Ramkumar, "Passive copy-move forgery detection using SIFT, HOG and SURF features," 2016 *IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, 2016, pp. 706-710.

[6] S. Prasad and B. Ramkumar, "Passive copy-move forgery detection using SIFT, HOG and SURF features," 2016 *IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, 2016, pp. 706-710.

[7] Weiqi Luo, Jiwu Huang and Guoping Qiu, "Robust Detection of Region-Duplication Forgery in Digital Image," *18th International Conference on Pattern Recognition (ICPR'06)*, Hong Kong, 2006, pp. 746-749.

[8] Zheng, J., Liu, Y., Ren, J. et al. Multidim Syst Sign Process (2016) 27: 989.

[9] M. R. Resmi and S. Vishnukumar, "A novel segmentation based copy-move forgery detection in digital images," 2017 *International Conference on Networks & Advances in Computational Technologies (NetACT)*, Thiruvananthapuram, 2017, pp. 346-350.

[10] S. Debbarma, A. B. Singh and K. M. Singh, "Keypoints based copy-move forgery detection of digital images," 2014 *International Conference on Informatics, Electronics & Vision (ICIEV)*, Dhaka, 2014, pp. 1-5.

[11] M. M. Isaac and M. Wilscy, "A key point based copy-move forgery detection using HOG features," 2016 *International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Nagercoil, 2016, pp. 1-6.

[12] Ryu SJ., Lee MJ., Lee HK. (2010) Detection of Copy-Rotate-Move Forgery Using Zernike Moments. In: Böhme R., Fong P.W.L., Safavi-Naini R. (eds) Information Hiding. IH 2010. *Lecture Notes in Computer Science*, vol 6387. Springer, Berlin, Heidelberg.

[13] Ilea, D., Whelan, P.: 'The stationary wavelet transform and some statistical applications'. *Lecture Notes in Statistics*, New York, 1995.

[14] Amerini, Irene, Lamberto Balian, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. "A sift-based forensic method for copy-move attack detection and transformation recovery", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3 ,pp. 1099-1110, 2011.

[15] M. F. Hashmi, A. R. Hambarde and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," 2013 *13th International Conference on Intellient Systems Design and Applications*, Bangi, 2013, pp. 188-193.